MITCHELL | HAMLINE School of Law

William Mitchell Law Review

Volume 35
Issue 5 *Journal of the National Security Forum*

Article 3

2009

Responses to Ten Questions

Marion "Spike" Bowman

RESPONSES TO THE TEN QUESTIONS

Marion "Spike" Bowman†

1. Do Americans need to give up their privacy to be safer?

Emphatically, the answer to that question is "no," but the question appears to assume an "either-or" condition. Privacy and security can co-exist—thanks to increasingly sophisticated technology. That a tension exists between privacy and security is unarguable, but it is a tension that is often emotional and increasingly artificial. Advances in technology give us an increasing capability to discover Non-Obvious Relationships (NOR) among the billions of data points discoverable in the ordinary records created by every-day life.

The argument that aggregating this data makes abuse more likely is not only emotional and artificial, it is also dysfunctional. It is emotional and artificial because both technical and regulatory safeguards are easily crafted. It is dysfunctional because technology has given the criminals, spies, and terrorists the ability to hide in cyber space and live "under the radar." Without aggregation of data and applying technology to discover NOR, the risk to Americans will increase.

Americans really do have privacy with respect to the Government, but the arrival of the digital age means that privacy, per se, is antediluvian because private industry goes where the Government does not. The means to protect personal information, regardless of where it resides, should be the benchmark issue.

Everything Americans touch, buy, attend, visit, or watch leaves a footprint. There is a record, somewhere, about nearly everything Americans and what most aliens do. Those records are of great benefit to industry, but they would be of great benefit as well for

---

† Mr. Bowman recently retired from his position as the Deputy, National Counterintelligence Executive. Mr. Bowman is a retired U.S. Navy Captain and is also retired from the Senior Executive Service of the Federal Bureau of Investigation. The views expressed in this article are his alone and do not imply endorsement of the U.S. Navy, the Federal Bureau of Investigation, the Office of the Director of National Intelligence, or any other U.S. Government agency.

people who wish to do Americans harm, whether foreign or domestic; therefore, it is essential that those records be safeguarded to protect Americans. However, safeguarding does not mean protecting from discovery. It means protecting the information that will be discovered. The footprints we leave behind are already collected and aggregated, and that personal information can be made available for sale. ChoicePoint and Amazon are two examples of data aggregators of personal information.

Few have yet to receive an e-mail from Amazon with the message that "We've noticed that readers who have purchased [insert a book title or author] have also purchased [insert any number of book titles]." Amazon tracks your reading habits for marketing purposes. ChoicePoint is a different sort of aggregator.

ChoicePoint is a Georgia-based company that combines personal data sourced from multiple public and private databases and makes that data available for sale to the Government and the private sector. The firm maintains more than 17 billion records of individuals and businesses, which it sells to an estimated 100,000 clients, including 7000 federal, state, and local law enforcement agencies.[1] While ChoicePoint sells data responsibly, it has suffered several security breaches that have led to the theft of the personal information it holds. The company has been criticized as much for the way it has handled the thefts as the incidents themselves. Its actions concerning a substantial breach in 2004 led to calls for new national privacy laws in the United States to protect the personal data of Americans. Since then, reports published in the media say that the company has improved its privacy practices.

It is simple reality to state that the greatest restrictions on discovery of private information about Americans are on the Government. With that in mind, let's return to the NOR problem. Changes in national security policy in response to the September 11 terrorist attacks boosted the role of ChoicePoint and other private companies that focus on sales to homeland security and crime-fighting agencies. Billions have gone to ChoicePoint and other private companies to gather intelligence information that is vital to protecting our citizens.

Why has all this money gone to private companies? Simply put, private companies can and do compile and use information in

1. These estimates are from March 30, 2005.

ways that government officials cannot. U.S. privacy and information laws strictly limit the Government's ability to collect information about U.S. citizens, but these restrictions do not apply to corporations.

As part of its national security contract work, ChoicePoint provided not only its commercially available products, but also, recognizing a business case for doing so, developed new information surveillance technology. According to 2003 federal contract documents released pursuant to Freedom of Information Act requests, that technology was used to identify terrorism by continuously tracking subjects of interest and providing electronic notification when new information became available.

Beyond cavil, ChoicePoint has provided an anti-terrorism service to the United States, but it is a clumsy sort of service. The information is not collected pursuant to any guidelines, it can be sold as any merchandise could be sold, and it is a cumbersome mechanism when, at least for counterterrorism purposes, speed is of the essence. The answer, not well received by the privacy lobby content to wear blinders, would be to permit the Government to collect and to aggregate data and use technology that provides the security and privacy that people believe they should have.

However, if ChoicePoint is not a compelling reason to let the Government aggregate personal data, consider cybercrime. It is a fact that substantially more of our information is public than we realize. There is a growing security threat posed by the massive amount of personal information posted on social networks, forums, blogs, and other Web 2.0 destinations. Consider, for example, how often we might use a mother's maiden name as a security clue. With permission, an individual recently accessed a friend's bank account in only an hour and a half after mining her personal blog for details like her birth date, birthplace, father's middle name, and pet's name. He used the data to reset her e-mail password and gain access to an e-mail from her bank with instructions on how to reset her account password.[2] Today, cybercriminals are increasingly mining personal data splashed throughout the Web 2.0 world.

Let me end this argument with an observation and a question. The events of September 11 are indelibly embedded in our minds and many arguments were made that chances to stop the attacks

2. Herbert H. Thompson, *How I Stole Someone's Identity*, SCI. AM., Aug. 18, 2008, http://www.sciam.com/article.cfm?id=anatomy-of-a-social-hack.

were missed—the dots were not connected. Given the law and the data available at the time, I do not believe that to be true. However, had the laws and systems been different, the events of September 11 might have been avoided. Consider the fact that two of the hijackers were known to be in the United States. Using only those two as a starting point, had it been possible to correlate addresses, frequent flyer numbers, telephone numbers, etc., all nineteen could have been identified with a simple link analysis program.

In 1979, the Supreme Court held that third party information is not constitutionally protected.[3] To what extent, then, would the Government's linking of information already public or voluntarily provided to third parties, without restriction, violate privacy?

6. For purposes of the Foreign Intelligence Surveillance Act (FISA), should Congress (re)erect a wall between criminal justice and foreign intelligence at the FBI?

First, let me point out that the question may be read to assume an incorrect fact. Congress never did erect a wall between criminal and intelligence information—the Department of Justice cut that wall from whole cloth and steadily grew it higher throughout the years. Congress, in the PATRIOT Act, affirmed a FISA appellate court's decision that no such barrier was ever intended. However, for the sake of the principle itself, I propose an emphatic "NO!"

Even a casual look back in time reveals that issues of national security and the social compact of the Constitution have begun to converge—and sharply so. Since the late 1970s, there has been more economic and traditional espionage activity and, more recently, the deadly threat of terrorism. These are not common crimes, susceptible to normal criminal techniques of coercion and/or punishment. These dangers strike at the heart of national and individual security, and they pose a very separate and distinct problem from that of the common thief. Whether the threat is loss of military advantage, terrorism, or the economic health of the Nation, these threats demand prevention rather than prosecution. More to the point, experience shows that prevention depends very heavily on the ability to conduct surreptitious surveillance and to collate all available information.

3. *See* Smith v. Maryland, 442 U.S. 735, 744–46 (1979).

National security threats are unlike common crime. What makes them more difficult is that they often arise in the context of converging First, Fourth, and, occasionally, Fifth Amendment protections. In practice, this means that probable cause requirements for obtaining surveillance authority is not "a fair probability that contraband or evidence of a crime will be found in a particular place." That standard does not mesh well with the needs of society when less obvious threats to national security are at stake. Rather, probable cause must relate to the target's status, i.e., a foreign power or an agent of a foreign power. As Justice Powell noted in the *Keith*[4] case, the fundamental distinction has to do with foreign influence, not domestic crime.[5]

However, the fact that foreign influence and domestic crime can be distinguished in theory does not mean they are not related in fact. Consider the terrorism cases tried in this country. With only a few exceptions, all of the defendants stood on the dock for criminal behavior, not for having committed terrorist acts. Some were guilty of conspiracy, some for illegal financial transactions, and some for credit card fraud. As a real and concrete example, the intelligence agent following a terrorist lead should have available to him the information that the criminal agent has developed from cigarette smuggling.

What this means in practice is that the intelligence investigator will compile more private information than a criminal investigator might compile because he has the benefit of both avenues of investigation. We tend to have a knee-jerk reaction that something is wrong with this. However, we need to consider what it means to fail to prevent the threatened activities—and we have a data point for that. When the Nation was young, when it was at war, when it was threatened, privacy was less important than security. When the Cold War ended and we were in a more secure environment, privacy clearly became increasingly important to "the people," and court decisions reflected those concerns. However, the law that emerged from *Keith* and its progeny, and eventually from Congress in the form of FISA, reflects the importance of knowing both the origins and nature of the threats to national security.

In our jurisprudence, we have a need to try to make legal argument and decisions fit into the molds of our prior experience.

4. United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297 (1972).
5. *Id.* at 308-09.

With the technologies in use today, this can be a vain attempt. Even if we can satisfy ourselves on an issue of search versus surveillance in a computer (and that is not a trivial issue), we are left with a bewildering array of new technologies that leave both traditional and evolutionary treatments of the Fourth Amendment in the dust.

Wireless communications, Voice Over Internet Protocol, steganography,[6] multiplexed data transmissions, and virtual worlds are simply indicators of what is to come. To expect that the public can be protected with decades-old methodology and thought processes is insane considering today's computer-based technology that enhances the terrorism threat; technology that becomes obsolete in around ninety days. To protect the public, law enforcement and intelligence officers will have to have tools that the privacy lobby will consider intrusive, including the ability to draw on information from both spheres.

The response should not be a knee-jerk, anti-investigative reaction. Rather, the response should be, as it was after the Church Committee, to work with the world as it exists, not as we might like it to be. Build the safeguards that meet the needs. Use technological advances not only to search out and compile information, but to protect privacy as well. Demand that congressional and executive branch oversight mechanisms move into the twenty-first century along with the technology.

In a prior age, these matters could proceed at a deliberate pace. Today, the advances in technology occur so rapidly, and the threats to national security are so dire, that both the means to combat the threat and the means to ensure privacy protection must develop quickly and together. The only security a "wall" provides is for those who would do us harm.

8. Is global warming a threat to American national security?

Yes! It would be far easier to stop right there than succinctly run through the implications for national security of a changing climate.

6. Steganography is hiding a secret message within a larger one in such a way that others cannot discern the presence or contents of the hidden message. For example, a message might be hidden within an image by changing the least significant bits to be the message bits. Today we think of this as the ability to fill, for example, all the unused bits of a graphic image (such as the American Eagle) with a secret message.

Although environmental issues have not had a significant effect on the United States, *Trail Smelter*[7] provides an example of how hard it is to settle cases between nations. In *Trail Smelter*, acid rain caused by a smelter near the Canadian border was causing agricultural and livestock damage in the United States. International arbitration went against Canada and compensation was disbursed over a period of years with some small residual amount being returned to Canada.[8] However, in 2003 the smelter issue arose again.[9] This time it was not acid rain; rather the smelter was dumping into a river that runs through the state of Washington before emptying into Lake Roosevelt, generating unsafe levels of toxins in fish and significant contamination along the banks.

The smelter had been dumping slag in the river everyday for sixty years. When the Environmental Protection Agency (EPA) tried to intervene, the company responded that they would offer thirteen million dollars for a study. The EPA countered with a request for full control at which point the company noted that it had a permit to dump and owed no obligation to U.S. law. This time the problem was intractable, and, in 2004, the Canadian Government quietly asked the United States to "back off."[10]

Obviously, Canada and the United States will not have a major conflict over this situation, but it illustrates how difficult it is to control transnational environmental issues. Meanwhile, the past few years have seen the climate vary from the norm, precipitating unusual heat in Europe, drought in the horn of Africa, alarming glacial melt, and an increase in water-borne disease. Whether true global climate change is occurring is not yet provable, but scientific estimates do suggest that the world is, as a whole, warming.

Already we have seen calls for action that could affect national security. For example, during the Burma crisis in 2008 there were calls to displace the ruling junta. Who knows what would have happened had the United States not been engaged in Afghanistan and Iraq; U.S. allies were quietly calling for displacing the junta but

7. Trail Smelter Arbitration Tribunal (U.S. v. Can.), 3 R. Int'l Arb. Awards 1911 (1938); *see also* Michael J. Robinson-Dorn, *The Trail Smelter: Is What's Past Prologue? EPA Blazes a New Trail for CERCLA*, 14 N.Y.U. ENVTL. L.J. 233, 235-41 (2006).

8. Robinson-Dorn, *supra* note 7, at 243-54.

9. *Id.* at 268-73.

10. *Id.* A significant problem in Europe involves the river systems that flow through many countries (e.g., the Danube) and determining what responsibilities are owed by upstream nations to downstream nations.

the logistical strength of the United States was not available. For the sake of argument, let's assume climate change will occur, and not for the better. What, then, does that mean for national security?

First, establishing some common ground is useful. Clearly, we can all agree that we live in a post-globalization, interdependent world. Few nations today have sufficient independent resources or economic production to survive solely within their own borders. More controversial is the postulation that instability in any nation threatens us all. However, national instability threatens regional stability and regional stability is fodder for a legion of harms.

A brief example is the implosion of the Soviet Union. A bevy of suddenly independent states with no political memory of democracy loosed massive official corruption and created breeding grounds for organized crime that still require international attention.[11] Ethnic tensions in the former Yugoslavia then led to massive "ethnic cleansing." A more poignant example is Darfur. There, intra-state conflict has given rise to corruption, weapons proliferation, terrorist training camps, and genocide. A cause of the chaos in Darfur is insufficient water resources for both the African and the Arab inhabitants of the region. Regional forces have been inadequate to control the situation, and United Nations personnel have been denied entry.

What then may we expect from climate change? First, the predicted climate change will exacerbate existing environmental crises such as drought, and soil degradation; it will intensify land-use conflicts and trigger environmentally induced migration. Sea-level rise, increased hurricane and flood frequencies could threaten coastal cities and industrial regions in China, India, and the United States. Melting glaciers would jeopardize water supply in the Andean and Himalayan regions. Glacier melt in the Himalayas, if continued at its current level, could dry up the Ganges River within fifty years. Andean glacier melt has decreased the size of the glacial fields 30% since 1974. (Interestingly, glacier ice on Mount Shasta in the United States seems to be growing.)

Vexingly, in some regions, too much water will be the problem. Already, water-borne diseases are increasing rapidly. The

11. The fastest growing organized criminal activity is unlawful disposal of hazardous waste. The loose controls of the newly independent states allowed this to develop quickly.

World Health Organization estimates that 150,000 die each year from climatic changes, the bulk from water-borne diseases (although some 20,000 Europeans died in 2004 from the heat). Twenty known diseases in general remission have re-emerged, including a virulent form of tuberculosis, malaria, and cholera.

Global warming is predicted to be 2–4°C, a range that will likely reduce agricultural productivity worldwide. If predictions hold true there will be desertification, soil salinization, and water scarcity. In South Asia and North Africa, where agricultural lands are already largely exploited, regional food crises will almost certainly undermine the economic performance of weak and unstable states.

Countries likely to suffer the greatest water stress are generally those that already lack the political and institutional framework necessary for the adaptation of water and crisis management systems. This could overstretch existing conflict resolution mechanisms, ultimately leading to destabilization and violence, the like of which we have already seen in Darfur. Weak governance structures and conflict are features of weak and fragile states. Food and water crises will likely result in permanent weakening or even dissolution of their state structures. Climate change could thus lead to the further proliferation of weak and fragile states and increase the probability of violent conflicts occurring.

We already know that migration can greatly increase the likelihood of conflict in transit and target regions. If climate change does prompt drought, soil degradation, and water scarcity, regions with high population growth will undoubtedly see significant migration. Most environmental migration will initially occur within national borders, but Europe and North America must also expect substantially increased migratory pressure from regions most at risk from climate change. States that will have to bear the costs of environmentally induced migration in the future will likely also have to guard against or engage in conflict. As environmental migration occurs, border areas are particularly likely to be areas of conflict. As we have seen repeatedly, even today, all of these pressures are likely to lead to significant human rights violations.

What this will mean for the future is unknown, but the likelihood of establishing a global governance structure to accommodate these pressures is poor. Climate change will disrupt economies worldwide, and globalization will exacerbate economic

problems well beyond national borders. Instability will call for interventions—likely both in the form of humanitarian assistance and military stabilization forces.

These issues were studied recently at the United States Army War College. The results of that study were striking. First, the study noted that the United States will have to integrate climate change into national security and defense strategies. Second, the significant logistical strength of the United States, coupled with superior military capabilities, will mean that we have to take a stronger role in stabilizing the change. Third, in order to preclude significant conflict, the United States should commit to global partnerships to aid less stable regions. Fourth, we must accelerate business practices and new technology to improve energy efficient combat power. Finally, we have to prepare for the future by assessing the impact of global change on militaries worldwide over the next thirty to forty years.

10. What is the most important issue for American national security?

I am a government employee writing in the waning months of the Bush administration and am about to make a heretical statement. The most important issue in national security is not terrorism—it is organized crime, defined to include economic and industrial espionage.[12]

In 1946, 56 nations signed the United Nations Charter. Today there are 193 nations in the world (depending on who is doing the counting), and an alarming number are weak, failing, or failed states. To take their place in the world they need to progress economically, and it is a simple fact that economic information is valuable. More than 100 nations and countless individuals and organizations are actively targeting our private industry for proprietary information.

Let's start with a few examples. Semion Mogilevich is a Russian crime boss who, among other frauds, headed a multi-million dollar scheme to defraud investors. Investors who owned stock of YBM Magnex International, Inc. lost more than 150 million dollars because of his scheme that included inflating stock values,

12. A close second would be energy. I chose organized crime because I believe that, even if Middle Eastern oil reserves are as low as some claim, there are sufficient oil reserves for a long enough period to develop alternate energy sources.

preparing bogus financial books and records, lying to the U.S. Securities and Exchange Commission officials, and offering bribes to accountants. This is just one example of many such frauds.

Chi-Mak and his wife Rebecca Chu were sent to the United States more than two decades ago to be "sleeper agents" on behalf of the People's Republic of China. They obtained citizenship, and Chi-Mak went into the defense industry. Over the years, he was tasked to provide unclassified, cutting-edge Research and Development information on defense work. He compromised, among other matters, submarine quieting technology and the Aegis radar system.

On June 17, 2008, experts from the automotive, pharmaceutical, and product safety industries told a U.S. Senate panel that counterfeit and pirated goods cost the U.S. economy billions of dollars and jeopardize the safety of consumers. According to Senator Patrick Leahy, a Democrat from Vermont and chairman of the Senate Judiciary Committee that is probing the issue, the losses from intellectual property alone robs the U.S. economy of at least 200 billion dollars and 750,000 jobs every year.

Organized crime is so lucrative that it can suborn our law enforcement officials. All too often, the money has tempted customs officers who wave in vehicles filled with illegal immigrants, drugs, or other contraband. Another Border Patrol agent may act as a scout for smugglers. But Customs and Border Patrol are not unique. Trusted officers of many agencies can fall prey to temptation and begin taking bribes if they have something organized crime wants.

Online crime simply follows the obvious—it gravitates to the money, and where money is in transit, it is vulnerable. And where the risk to the criminal is lowest is where the criminal is going to go. Online hacking is increasingly motivated by money. It could be corporate espionage or organized crime. There is more money in organized cybercrime than there is in drugs, and many cartels are switching from drugs to cybercrime, because the risk is less, the capital investment is smaller, and it's almost anonymous. You don't have to stand in the "line of fire." As more ready-made tools become available, and more people transact and communicate online, the value proposition for industrial espionage, organized crime, and intelligence gathering becomes increasingly favorable.

Even with a Gross Domestic Product estimated at 13.8 trillion dollars in 2007, the economic health of the Nation is imperiled by

organized crime, whether it is generated by groups or nations. Information is valuable and not just that which is related to military and defense industries. The formulas that go into making bullet proof vests, cholesterol medications, and surgical adhesives cost millions, often hundreds of millions, to develop. Stealing information like that is big business; corporate America is at risk, and the economic health of the Nation is rapidly deteriorating. Recognizing this phenomenon, on April 23, 2008, the Department of Justice made the following announcement:

> Today, Attorney General Michael B. Mukasey announced a new strategy in the fight against international organized crime that will address this growing threat to U.S. security and stability. The Law Enforcement Strategy to Combat International Organized Crime . . . was developed following an October 2007 International Organized Crime Threat Assessment . . . and will address the demand for a strategic, targeted, and concerted U.S. response to combat the identified threats. This strategy builds on the broad foundation the Administration has developed in recent years to enhance information sharing, and to secure U.S. borders and financial systems from a variety of transnational threats.[13]

This will not be easy. Today, the FBI is struggling to get enough manpower to police common crimes. FBI resources for non-terrorism cases are so depleted that corporations complain that they can't get authorities to pay attention to frauds running into millions of dollars. Statistics are difficult to compile, but one assessment is that prosecutions of frauds against financial institutions dropped 48% from 2000 to 2007, insurance fraud cases plummeted 75%, and securities fraud cases dropped 17%. Another report shows a deep decline of 50% for all white-collar crimes. In the long run, the economic health of the country is our greatest national asset, and we are not protecting it well.

13. Press Release, Dep't of Justice, Dep't of Justice Launches New Law Enforcement Strategy to Combat Increasing Threat of Int'l Organized Crime (Apr. 23, 2008), http://www.usdoj.gov/opa/pr/2008/April/08-opa-330.html.